Cryptography Using Congruences

Math 502 Supplement

February 20, 2006

Maple handles strings as a *type*. There is two-way conversion of strings to lists of numbers (based on character ASCII codes):

```
> s := "And then it started like a guilty thing upon a fearful summons.":
> v := convert(s,'bytes'):
> nops(v);
                                       63
> op(1,v), op(2,v), op(63,v);
                                   65, 110, 46
> convert(v,'bytes');
       "And then it started like a guilty thing upon a fearful summons."
```

Congruence-based cryptography treats these number lists as lists of numbers modulo m for some suitably large modulus m. One takes some large power of each number in a number list. Encryption is enabled when one finds a *pair* (d, e) of these exponents for a given m such that the operation of taking the e-th power inverts the operation of taking the d-th power.

```
> pm := (x,m,k) -> x &^ k mod m:
> pm(257,19781,41);
                                      19128
> pm(19128,19781,761);
                                       257
```

For the modulus $m = 19781$ the pair $(d, e) = (761, 41)$ is a pair of such exponents.

```
> w:=map(pm,v,19781,41):
>  nops(w);
                                       63
> op(1,w), op(2,w), op(63,w);
                               6727, 18700, 10230
> vv:=map(pm,w,19781,761):
> convert(vv,'bytes');
       "And then it started like a guilty thing upon a fearful summons."
```

The 95 printable ASCII codes have values in the range from 32 to 126 (hexadecimal 20 – 7E). If one works with these as unencoded numeric values, one will then want any prime factor of m to be larger than 126. Consider the case where m is a prime p. By Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$ for each $a \not\equiv 0 \pmod{p}$, or $a^p \equiv a \pmod{p}$ for all a. It follows that if $r \equiv s \pmod{p-1}$ and $r, s \geq 0$, then $a^r \equiv a^s \pmod{p}$ for all a. In the case that $m = p$ is prime, one wants a pair (d, e) such that $de \equiv 1 \pmod{p-1}$. This makes it necessary that d, e both be coprime to $p - 1$. For a given e that is coprime to $p - 1$ there is a unique such d mod $p - 1$.

For example, with $m = p = 131$, one has $p - 1 = 130 = 2 \cdot 5 \cdot 13$. Then $e = 77 = 7 \cdot 11$ is coprime to $p - 1$.

```
> msolve(77*x=1,130);
                                    {x = 103}
```

Therefore, $d = 103$ may be paired with $e = 77$ when working mod 131.

This generalizes to the case where $m = p_1 \dots p_n$ is the product of distinct primes $p_1, \dots, p_n$. In this case a congruence mod m is equivalent to simultaneous congruences modulo each of the primes p_j. Thus, with $u = \mathrm{lcm}(p_1 - 1, \dots, p_n - 1)$ if $r \equiv s \pmod{u}$ and $r, s \geq 0$, then $a^r \equiv a^s \pmod{m}$ for all a. Thus, for a given e that is coprime to u one finds d as the unique solution of the congruence $ex \equiv 1 \pmod{u}$.